Social Transformations in Contemporary Society, 2018 (6)
ISSN 2345-0126 (online)

USERS ELECTRONIC DATA PROTECTION FEATURES

Aurimas Šidlauskas

Mykolas Romeris University, Lithuania
aurimas868@gmail.com

Abstract

Purpose – to analyze the peculiarities of users electronic data security and to propose recommendations that would reduce the risk of data loss and misuse.

Design/methodology/approach – analysis and study of scientific literature, comparison, the main features complex generalization, induction methods.

Finding – after analyzing the theoretical aspects of users electronic data protection features, there were introduced the main recommendations that would reduce the risk of data loss and misuse.

Research limitations/implications – would be necessary to do a bigger research and apply more methods.

Practical implications – this information can be used to enhance security measures to avoid incidents involving loss, alteration, and misuse of data.

Originality/Value – cyber security is the most critical aspect nowadays of our technologically based lives. Neglected the protection of electronic data, highlighted the complex security components: poor (weak) passwords used, irresponsible sharing of private information on social networks with third parties.

Keywords: electronic information, CIA triad, passwords, authentication, Facebook social network, data security.

Research type: general review.

Introduction

The ever-growing use of technology encourages a wide range of security measures to protect consumers' electronic data.

Information security (safety) is understood as the protection of information and system infrastructure against accidental or intentional, natural or artificial effects that could cause damage to the owners or users of the information or system infrastructure in question (Štitilis et al., 2016). Information security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security countermeasures of all available types (technical, organisational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats (Cherdantseva, Hilton, 2013). Information security issues of a technical nature have been prevalent for a long time and are still relevant, but there is has been an obvious and ongoing shift in the problems investigated in

ISSN 2345-0126 (online)

information security research towards a wider, increasingly more multi-faceted managerial approach (Jastiuginas, 2012).

Object of the research. Electronic data security.

Purpose – to analyze the peculiarities of users electronic data security and to propose recommendations that would reduce the risk of data loss and misuse.

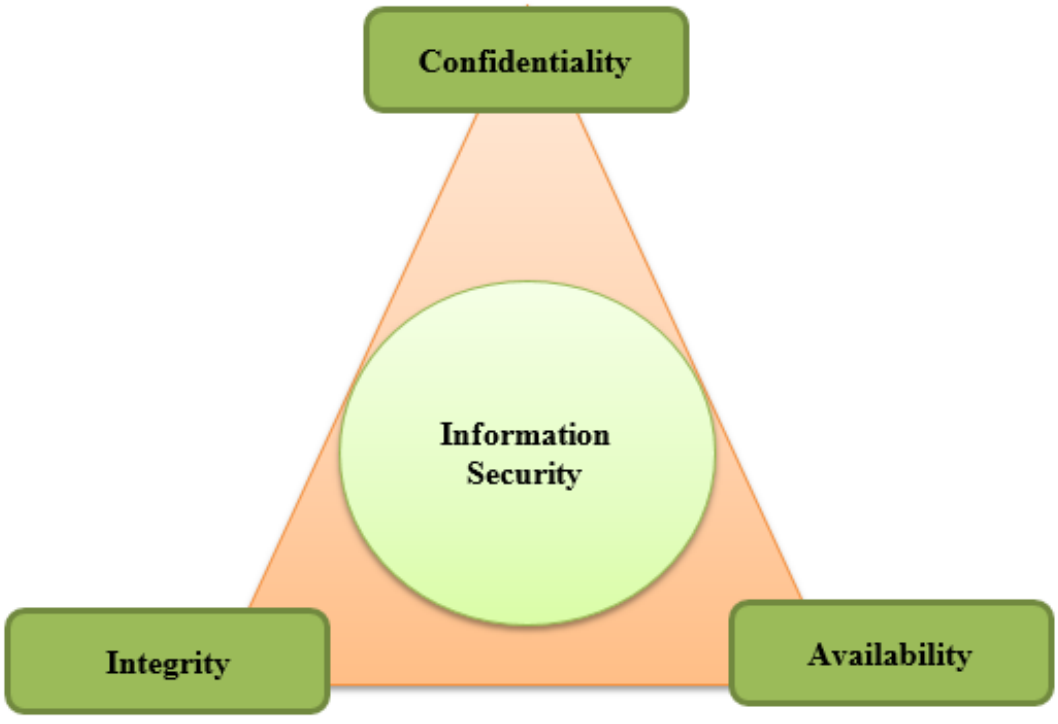
There have been set the following objectives for the above mentioned purpose to be achieved to:

1. Set the impacts, potential consequences and methods of control of confidentiality, integrity and availability;
2. Evaluate random passwords to determine their security;
3. Determine Facebook authentication features.

Data is information that a computer receives, processes, displays and stores. Data is divided into images, texts, numbers, symbols and characters. Data is converted into information when it becomes understandable to a particular entity. Often, data and information are considered synonymous. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction (Andress, 2011). Data (information) security is a global, continuous process that requires continuous improvement in adapting to changing technologies.

CIA triad analysis

The Security triad or CIA triad, a distinguished model for the development of security mechanisms, implements the security by making use of the three areas which are Data confidentiality, integrity and availability (Farooq et al., 2015) as shown in the Fig. 1.



Source: Author

Figure 1. CIA triad model

ISSN 2345-0126 (online)

The three core goals have distinct requirements and processes within each other:

1. Confidentiality is the protection of information from unauthorized access or disclosure.

2. Integrity is the protection of information from unauthorized modification;

3. Availability ensures the timely and reliable access to and use of information and systems.

Confidentiality is approximately equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. Access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.

Integrity involves maintaining the accuracy, consistency, and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.

Availability ensured by the maintenance of hardware as well as maintaining the operating system in proper functioning where any kind of software conflict doesn't take place (Mohanty et al., 2018). It's also important to keep current with all necessary system upgrades.

The CIA triad of information security was created to provide a baseline standard for evaluating and implementing information security regardless of the underlying system and/or organization. A breach in any of these areas could cause serious issues to the system. The impacts, potential consequences and methods of control of confidentiality, integrity and availability are shown in Table 1.

Table 1. Confidentiality, Integrity and Availability Model and Related Impacts

Requirement	Impact and Potential Consequences	Methods of Control
Confidentiality: the protection of information from unauthorized disclosure	Loss of confidentiality can result in the following consequences: • Disclosure of information protected by privacy laws • Loss of public confidence • Loss of competitive advantage • Legal action against the enterprise • Interference with national security	Confidentiality can be preserved using the following methods: • Access Controls • File Permissions • Encryption
Integrity: the accuracy and completeness of information in accordance with business values and expectations	Loss of integrity can result in the following consequences: • Inaccuracy • Erroneous decisions • Fraud	Integrity can be preserved using the following methods: • Access controls • Logging • Digital Signatures • Hashes • Encryptions

ISSN 2345-0126 (online)

Requirement	Impact and Potential Consequences	Methods of Control
Availability: the ability to access information and resources required by the business process following consequences	Loss of availability can result in the following consequences: • Loss of functionality and operational effectiveness • Loss of productive time • Interference with enterprise's Objectives	Availability can be reserved using the following methods: • Redundancy • Backups • Access Controls

Source: Isaca, 2015

Jastiuginas (2012) argues that technical measures alone are insufficient to ensure information security. Information security management includes three dimensions:

1. Strategic - administration, organization, management and compliance with standards, legal instruments and best practice;
2. Human - security culture, competence, training, psychological aspects;
3. Technological - hardware and software instruments.

Safeguarding information has been a priority for as long as people have needed to keep information secure and private.

Analysis of a secure system for password generation

In the physical world, the best analogy would be that any person can claim to be anyone (identification). To prove it (authentication), however, that person needs to provide some evidence, such as a driver's license, passport, and so forth (Dulaney, Easttom, 2014). The classic paradigm for authentication systems identifies three factors as the cornerstones of authentication:

1. Something you know (e.g., a password);
2. Something you have (e.g., an ID badge or a cryptographic key);
3. Something you are (e.g., a fingerprint or other biometric data).

Authentication -The act of verifying the identity of a user and the user's eligibility to access computerized information. Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.

Passwords are a traditional and widespread method of authentication, both on the Internet and off-line. Passwords are portable, easy to understand for laypersons, and easy to implement for the operator. Thus, password-based authentication is likely to stay for the foreseeable future. Most sites let users choose their password, as the usability of automatically generated passwords is low (Yan et al., 2004). Existing password-based authentication schemes can be categorized into two types - one uses weak password and the other uses strong-password (Das et al., 2004). A password is a string of characters used for authenticating a user on a computer system. Most passwords are comprised of several characters, which can typically include letters, numbers, and most symbols, but not spaces. Passwords play a large part of the typical web user's experience. They are the near universal means for gaining access to

ISSN 2345-0126 (online)

accounts of all kinds. Email, banks, portals, dating and social networking sites all require passwords. Text-based passwords are the most common mechanism for authenticating humans to computer systems. The more difficult a user's password is, the more difficult it becomes for a miscreant to break it and log in as that user, and the more difficult it becomes, as well, for the user to remember it. Thus, you need to obtain a fine balance between the two extremes. Passwords are the first line of defense against attacks to a computer system. The rules for password choice can be certainly a cumbersome problem for a user and a security problem for a system.

SANS (SysAdmin, Audit, Network, Security) is a large collaborative group of security professionals that provide information security training and certification. Their recommended password protection policy defines the standard for the creation of strong passwords.

1. Strong passwords have the following characteristics:

- Contain at least 12 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,./).

2. Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

Various organizations provide similar recommendations. Failure to comply with the recommendations for creating a secure password increases the risk of the system being hacked into and the password may be appropriated by a third party. There are many websites on the Internet where one may check the strength of the password and the time required to guess what it is. We have used "Kaspersky Lab secure password check" to check strong passwords created in accordance with the recommendations for secure password generation and insecure (short, memorable) passwords and obtained the following results (see Table 2):

ISSN 2345-0126 (online)

Table 2. Weak and strong passwords

Weak password	Brute force attack cracking time	Strong password	Brute force attack cracking time
Terminator	37 seconds	20'sTerm1nator!	15 years
Psychopath	2 minutes	Psy-cho*path	200 years
Oldhouse	17 minutes	1Old*/house2*	25 years
rockmusic	15 minutes	R0ck/*mu-sic	94 years
Internetas1	12 days	1nter/netaS*	30 years
darkroom	2 minutes	Daark/1room*	41 years

Source: Kaspersky Lab secure password check

In brute force attack, all possible combinations of password apply to break the password (Fujita, Hirakawa, 2008). A brute-force attack is an attempt to guess passwords until a successful guess occurs. For example a user enters a password of 8 characters and all characters are lower case letters then to break the password using the brute force attack it requires $(26)^8$ combinations which is equal to 208827064576.

US National Institute of Standards and Technology (NIST) Special Publication 800-63B states that users should be encouraged to make their passwords as lengthy as they want, within reason. Since the size of a hashed password is independent of its length, there is no reason not to permit the use of lengthy passwords (or pass phrases) if the user wishes. Extremely long passwords (perhaps megabytes in length) could conceivably require excessive processing time to hash, so it is reasonable to have some limit. It now suggests that users create passwords with long, easy-to-remember phrases.

A check of random long passwords on "Kaspersky Lab secure password check" has yielded the following results (see Table 3):

Table 3. Long passwords

Long passwords	Number of characters	Brute force attack cracking time
Ifeelgoodtonight*	17	4 centuries
Mycatisveryangry	16	11 centuries
Houseundertheground	19	4 centuries
Rock/metal*music	16	13 centuries
It.hastobedone	14	12 centuries
Neverending-story	17	4 centuries

Source: Kaspersky Lab secure password check

To summarize the results, one can argue that the length of the password and the characters used therein have a significant impact on security. Longer passwords comprised by individual words are safer and easier to remember than shorter passwords with multiple characters.

ISSN 2345-0126 (online)

Personal data security on the Facebook social networking platform

A social network is an online community of people with a common interest who use a website or other technologies to communicate with each other and share information, resources, etc. Facebook is the largest social network on the planet boasts an extremely large user base with a large number of groups for sharing interests. Facebook is also used to share comments on a multitude of websites, making its reach even farther (Oriyano, 2017). The popularity of social networks is constantly increasing. Facebook is the most popular social network in the world with a monthly number of active users of over 2 billion (Statista, 2018).

Specifically, updating profile information, posting status updates, sharing photos and videos, and commenting on others' posts - to name a few - are behaviors that reveal aspects of one's personal identity. However, this escalating personal exchange on social networking sites also raises questions about privacy risks and consequences (Fogel, Nehmad, 2009). In fact, social capital researchers suggest that people must be willing to reveal personal information in order to fully experience the relational benefits of social media use (Vitak, 2012). Most probably one of the great advantages of social networks is that they make the world more open and more interconnected. Not only distances between people disappear but also longer time needed to transfer the message, and users can communicate with other people in real time although they are on the different sides of globe.

Research shows that factors such as attitudes toward privacy, security, and transparency can impact online disclosure practices (Acquisti, Gross, 2006). Authors Limba and Šidlauskas (2018) states, what information users share with the Facebook social network is an individual choice, some of them alone provide a lot of information about themselves and the whole surrounding reality, and others strive to protect their privacy and publish only minimal information. Types of the user data publicity:

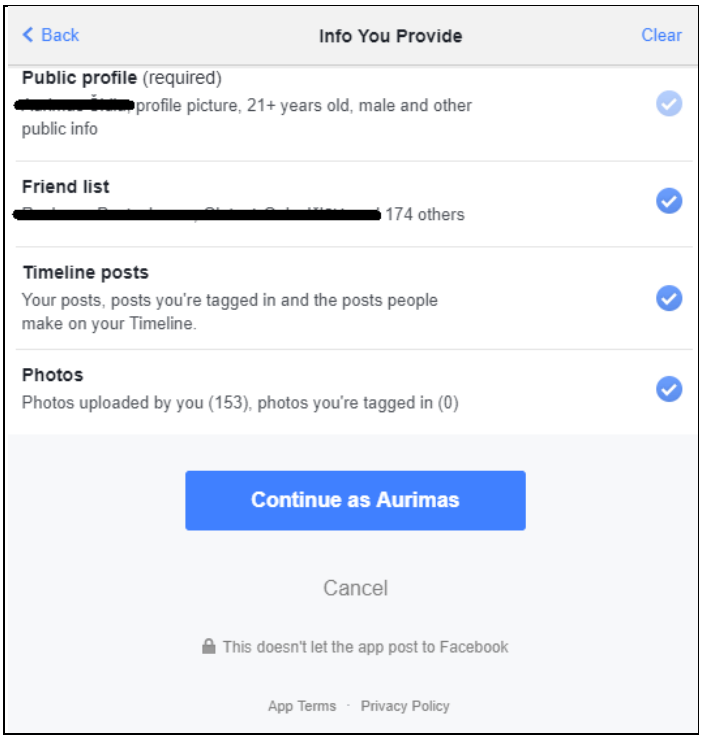
1. Public information, which is publicly available to all Facebook users;
2. Secret information, which is available only to the Facebook account administrator;
3. Closed information, which is publicly available to all Facebook users or individual friends and specific interest groups.

Various sites whose services are only available to registered users are increasingly offering an alternative form of registration: namely, authentication through sharing the user's personal data via the Facebook's social networking platform. Certain personal data is required for traditional user registration, including the login, the password or the email address. The specific personal data requested depends on the service provider on the nature of the the services in question. A user may be required to provide their name and surname, year of birth, telephone number etc. In order to login to a particular website, a user enters their login and password.

Registration via Facebook is a much faster way to connect to a website as one does not need to enter any of the data requested. The site authenticates the user on the basis of their Facebook data. The user must submit a public profile to a third party containing the following: name, profile picture, age range, gender, language, country, and other public information. Often, websites abuse this principle and ask for an unreasonable amount of personal data, such as the user's friend list, photos, email

ISSN 2345-0126 (online)

address, likes, birthday, timeline posts and other information. Below one can see the Facebook user authentication window (Figure 2).



Source: Facebook social network

Figure 2. Facebook user authentication window

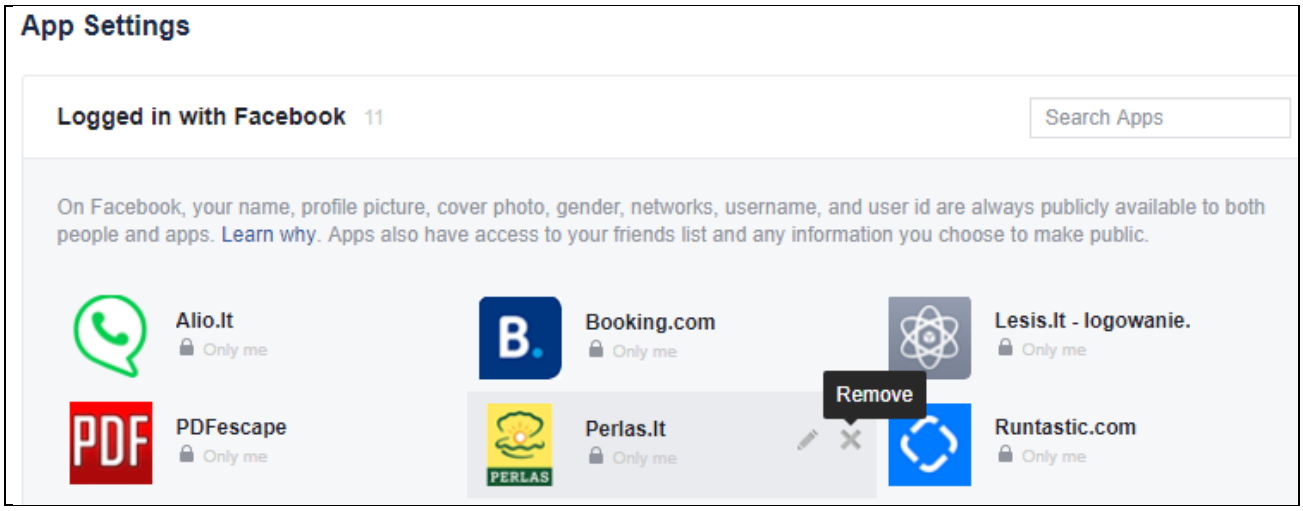
The user is able to edit the list of requested data and refuse to provide all the information, but the service provider may deny them access, in which case the desired service will be inaccessible. In this case, the user can re-register and submit the remaining requested data (Šidlauskas, 2017). Third-party provide social network user privacy policies that specify the terms that the user must accept prior to using the application. Privacy policies are often overlooked due to their complexity and scope. In this case, consumers become vulnerable because they do not know if their rights of personal data subjects are guaranteed. The main problem with the virtual social network Facebook, as well as other virtual social networks, is that the purpose of data collection and administration is either obscure or too broadly defined (Karg, Fahl, 2011).

In a similar vein, research in the area of information privacy also focuses on people's attitudes toward safeguarding their privacy at an institutional level as threats to privacy are largely associated with the desire for privacy protection (Lyon and Zureik, 1996). In light of the inundation of personal data revealed in the virtual world, the abundance of information that is freely and publicly shared by users is likely to promote a culture where both perceived threat to privacy and support for privacy protection are mitigated (Tsay-Vogel et al., 2016).

Scholars point to the negative implications of the disclosure of personal data as it is related to identity theft, harassment, cyberstalking, bullying, and unwarranted rumors and gossip (Tavani, Grodzinsky, 2002). On the other hand, although users

report being aware of privacy risks, they do little to implement safeguards to protect their personal information (Dwyer et al., 2007).

Once a user registers on a particular website through Facebook, an application is created and then entered into the user's Facebook profile. The site manager obtains permanent access to the user's Facebook data (verified during authentication). To ensure the security of their personal data, users should regularly view their Facebook settings and delete any applications they do not use. In this way, access to the user's personal data is discontinued for the third party (site) (see Figure 3).



Source: Facebook social network

Figure 3. Facebook App Settings

It is important to note that removing the application does not delete the data possessed by the third party. As a result, users who want their personal data to be deleted need to send a separate email to the site administrator, although one cannot guarantee that the user's data will actually be deleted after such a request.

Conclusions

Confidentiality, integrity and availability are the concepts most basic to information security. These concepts in the CIA triad must always be part of the core objectives of information security efforts. The CIA triad of information security was created to provide a baseline standard for evaluating and implementing information security regardless of the underlying system and/or organization. The factors relevant to information security are combined within the strategic, human and technological dimensions of information security management. Information is the greatest asset and the most important security object.

Authentication is the act of verifying the identity of a user and the user's eligibility to access computerized information. Passwords are a traditional and widespread method of authentication, both on the Internet and off-line. The length of a password and the characters used therein have a significant effect on security. Long passwords comprised by individual words are safer and easier to remember than shorter passwords with random characters.

To gain access to the services of certain registration-based websites, users must decide which mode of registration to use: traditional (user authentication using a login and password) or alternative (user authentication using data from a social networking platform). Registration through Facebook grants a third party (site manager) permanent access to the personal data on the user's social networking page that was verified during authentication, as the site's application is integrated into the user's Facebook profile. To ensure the security of their personal data, users should regularly review their Facebook settings and delete any applications they do not use. In this way, access to the user's personal data is discontinued for the third party (site).

References

Acquisti, A.; & Gross, R. 2006. Imagined communities: awareness, information sharing and privacy on Facebook. 6th workshop on privacy enhancing technologies, Cambridge, 28–30 June. https://doi.org/10.1007/11957454_3

Andress, J. 2011.The basics of information security: understanding the fundamentals of infosec in theory and practice. Waltham, MA: Syngress.

Cherdantseva, Y.; Hilton, J. 2013. Information Security and Information Assurance. Organizational, Legal, and Technological Dimensions of IS Administrator. IGI Global Publishin.

Das, L. M.; Saxena, A.; Gulati, P. V. 2004. A dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics 50(2): 629-631. https://doi.org/10.1109/TCE.2004.1309441

Dulaney, E.; & Easttom, C. 2014. Comptia Security+ Study Guide: Sy0-401, 6th Edition.

Dwyer, C.; Hiltz, S. R.; Passerini, K. 2007. Trust and privacy concern within social networking sites: a comparison of Facebook and MySpace. In: Proceedings of the thirteenth Americas conference on information systems, Keystone, CO, 31 December.

Facebook social network, 2018. Retrieved from https://www.facebook.com/

Farooq, U. M.; Waseem, M.; Khairi, A.; Mazhar, S. 2015. A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications 111(7): 1-6. https://doi.org/10.5120/19547-1280

Fogel, J.; & Nehmad, E. 2009. Internet social network communities: risk taking, trust, and privacy concerns, Computers in Human Behavior 25(1): 153-160. https://doi.org/10.1016/j.chb.2008.08.006

Fujita, K.; & Hirakawa, Y. 2008. A study of password authentication method against observing attacks. 6th International Symposium, Intelligent Systems and Informatics, SISY. https://doi.org/10.1109/SISY.2008.4664927

Yan, J. J.; Blackwell, F. A.; Anderson, J. R. 2004. Password memorability and security: Empirical results. IEEE Security & Privacy, 2(5): 25-31. https://doi.org/10.1109/MSP.2004.81

Isaca. 2015. Cybersecurity Fundamentals Study Guide. Information Systems Audit and Control Association

Jastiuginas, S. (2012). Integralus informacijos saugumo valdymo modelis. Informacijos mokslai, 61: 7-30.

Karg, M.; Fahl, C. 2011. Rechtsgrundlagen für den Datenschutz in sozialen Netzwerken. Komminakation und Recht 7(8): 456-458.

Kaspersky Lab: Secure Password Check. Retrieved from https://password.kaspersky.com/

Limba, T.; & Šidlauskas, A. 2018. Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook, Entrepreneurship and Sustainability Issues 5(3): 528-541 https://doi.org/10.9770/jesi.2018.5.3(9)

Lyon, D.; & Zureik, E. 1996. Surveillance, privacy, and the new technology. Computers, Surveillance, and Privacy. Minneapolis, MN: University of Minnesota Press.

Mohanty, S.; Ganguly, M.; Pattnaik, K. P. 2018. CIA Triad for Achieving Accountability in Cloud Computing Environment, International Journal of Computer Science and Mobile Applications 6(3): 38-43.

NIST Special Publication 800-63B. 2017. Digital Identity Guidelines: Authentication and Lifecycle Management. https://doi.org/10.6028/NIST.SP.800-63b

Oriyano, S. (2017). Certified Ethical Hacker Version 9 Study Guide. John Wiley & Sons. https://doi.org/10.1002/9781119419303.ch2

Sans.org, 2014. Consensus Policy Resource Community, Password Construction Guidelines. Retrieved from https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines

Statista.com, 2018. Number of social network users worldwide from 2010 to 2021 (in billions). Retrieved from https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Šidlauskas, A. 2017. Vartotojų elektroninių duomenų apsaugos ypatumai. Mykolo Romerio universitetas. Retrieved from https://elaba.lvb.lt:443/ELABA:LABTALL:ELABAETD25184230

Štitilis, D.; Kiškis, M.; Limba, T.; Rotomskis, I.; Agafonov, K.; Gulevičiūtė, G.; Panka, K. 2016. Internet and Technology Law. Vilnius: Mykolas Romeris universitety.

Tavani, H. T.; & Grodzinsky, F. S. 2002. Cyberstalking, personal privacy, and moral responsibility. Ethics and Information Technology 4: 123-132. https://doi.org/10.1023/A:1019927824326

Tsay-Vogel, M.; Shanahan, J.; Signorielli, N. 2016. Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. New Media & Society. 20(1): 141-161 https://doi.org/10.1177/1461444816660731

Vitak, J. 2012. The impact of context collapse and privacy on social network site disclosures. Journal of Broadcasting & Electronic Media 56: 451-470. http://dx.doi.org/10.1080/08838151.2012.732140